ASEAN Regional Forum
Cyber Incident Response Workshop
Republic of Singapore
6-7 September 2012

Co-Chair's Summary Report

1. Pursuant to the 18th ASEAN Regional Forum (ARF) Ministerial meeting in Bali, Indonesia, July 2011, the ARF Workshop on Cyber Incident Response was held on 6-7 September 2012 in Singapore. The workshop was co-chaired by Ms Aileen Chia of Singapore and Dr Carolyn Patteson of Australia.

2. The Workshop was attended by 68 participants with representatives from ASEAN Secretariat, Australia, Brunei Darussalam, Canada, the Delegation of the European Union to Singapore, Indonesia, Japan, Lao PDR, Malaysia, Mongolia, Myanmar, New Zealand, People's Republic of China, Philippines, Republic of Korea, Russian Federation, Singapore, Thailand and Vietnam.

Welcome and Opening Remarks

3. Singapore and Australia co-chaired the opening session of the workshop. In the opening remarks, the co-chairs noted that cyber-crime is one of the most significant threats faced by everyone and is a rapidly evolving and constant challenge. They recognised that it cannot be countered by any one organisation or country and required a partnership approach both nationally and internationally. They emphasised the need for everyone to work together in order to prevent and respond to cyber attacks, with the practical nature of this workshop designed to explore how to share information efficiently and effectively. The workshop also aims to develop participants' understanding of how to collaborate during a cyber security incident. The co-chairs then handed over to Dr Jason Smith and Mr David Campbell from CERT Australia to facilitate the rest of the workshop.

Workshop Aim and Objectives

4. Mr David Campbell provided participants with an overview of the aim and objectives for the workshop;

Aim - To develop participants' understanding of how ARF and sub-regional participants may collaborate in the event of a cyber security incident.

Objectives –

- Develop an understanding of the domestic arrangements of each participant, including the equivalency of offences and law enforcement powers and procedures;
- Understand and explore how to communicate and share information in the event of an incident;
- Identify models of best practise within the region, and
- Prioritise capacity building activities for those participants with less mature frameworks and mechanisms.

5. ARF members were invited to nominate up to four participants to take part in the workshop with delegations requested to include at least one working/operational level participant from the national computer emergency response team and one from an agency responsible for cyber crime/law enforcement. Participants were advised that the activity would be conducted as a discussion exercise.

Introduction to Discussion Exercise

6. Ms Lindl Rowe from CERT Australia explained the structure of the discussion exercise and the process for the day's activities to participants. Participants were advised the following:

- Facilitators will present the scenario and discussion questions to the whole group, each table group will then discuss the scenario and associated questions. An assistant facilitator will be seated at each table to aid with discussions and the lead facilitators will float around the floor during discussions to assist where needed.
- Following an allocated amount of time for each scenario, two table groups will be asked to present a summary of their table's discussions to the broader group. Different table groups will be asked to present after each scenario, with the facilitators also providing the opportunity for others to provide input amongst the larger group.
- Participants were also advised the context and assumptions used in developing the exercise and the ground rules for participants.

Scenario Discussions

7. **Scenario 1 – VOIP**
Mr David Campbell introduced the topic for the first scenario, and then handed over to Dr Jason Smith who presented the scenario and the factors/issues to consider during discussions. The complete VOIP scenario and discussion questions are at **Annex A**.

8. Throughout the table discussions, participants were assisted by a facilitator from Singapore at each table, as well as Dr Jason Smith, Mr Dave Campbell and Senior Sergeant Steve Honiss from the National Cyber Crime Centre - New Zealand Police, who floated amongst the tables during discussions.

9. Following the allocated discussion time, two table groups presented the outcomes of their discussion to the workshop.

10. **Scenario 2 – SCADA Vulnerability**
Mr David Campbell introduced the topic for the second scenario and explained the relevance of the scenario to participants, and then handed over to Dr Jason Smith who presented the scenario and the factors/issues to consider during discussions. The complete SCADA Vulnerability scenario and discussion questions are at **Annex B**.

11. Table groups were once again assisted by facilitators during their discussions, following which two different table groups presented the outcomes of their discussions to the workshop.

12. **Scenario 3 – DDOS**

Mr David Campbell introduced the topic for the third scenario, and then handed over to Dr Jason Smith who presented the scenario and the factors/issues to consider during discussions. The complete DDOS scenario and discussion questions are at **Annex C**.

13. Again, facilitators assisted the table group discussions with the last two table groups presenting the outcomes of their discussion to the workshop.

Key Observations

14. Throughout the scenario discussions, all facilitators took note of key observations that were raised by the groups. These observations were then summarised in to six key overarching observations with the detailed observations then grouped under five broad headings. The facilitators presented these observations to the participants and provided the opportunity for further discussions around these issues.

Key Overarching Observations

15. The six key overarching observations are:

- Information sharing is common once an incident has occurred. A challenge is how to reuse response processes and relationships to share information on threats before an incident occurs to improve preparedness and prevention. [Relates to all four workshop objectives - ALL]
- Participants from non-operational areas gained a better understanding of the challenges presented by these topics which will contribute to better informed policy developments. [Relates to all four workshop objectives - ALL]
- National level efforts are needed to coordinate and analyse sector or organisational specific views of the threat environment (that is, to build a national level picture of the threat). [Relates to objective four - CAPABILITY]
- Effective working relationships between national and international teams are essential, as is access to timely, high quality information. For particularly sensitive issues (such as SCADA vulnerabilities) CERT teams may not always have access to full information. [Relates to objective four - CAPABILITY]
- CERT and law enforcement processes and procedures are on the whole well aligned – law enforcement and CERTs work effectively together across the region. [Relates to objective one - ARRANGEMENTS]
- Challenges faced by regional participants might be similar, but laws and regulations vary across jurisdictions. Strong laws and regulations support timely and effective response. [Relates to objectives one and three - ARRANGEMENTS, PRACTICE]

Detailed Observations - Broad themes

16. A range of observations were captured and grouped under five broad themes as follows:

Governance (Policy Frameworks and Regulations)

- Regulations and policies may vary from country to country, particularly with respect to;
    - Definition of critical infrastructure
    - Mandatory reporting and metrics
    - Restrictions and requirements for connectivity to public networks, hardware and software used by critical infrastructure, etc.
- Some participants stated that prior to the workshop, they did not fully appreciate the current cyber security environment and the discussion exercise assisted them to gain a better understanding which will support their role in further development of policy frameworks and regulations
- Some countries are still developing specific cyber security legislation

Communications and Information Sharing

- Factors influencing ability to share information include:
    - Platform for sharing
    - Impact of incident
    - Resolution/mitigation readiness
- International information sharing does occur;
    - Via existing arrangements, for example ASEAN CERT/APCERT between CERT teams are available
    - International sharing may make use of many channels, including CERTs , LEAs/Interpol, diplomatic channels or bilateral arrangements
    - Some countries may be more reluctant to share information internationally than domestically and may have requirements that must be satisfied before information is shared (for example, require a formal request from a victim country)
- Majority of participants identified that media responses to threats from issue motivated groups were only provided after an incident

Inter-agency Collaboration

- CERT and LEAs do work together though powers and responsibilities may vary based on jurisdiction
- Appetite for greater international information sharing across CERTs and LEAs – technical insights and intelligence in particular and for sharing best practices to ensure that actions do not disrupt legitimate, ongoing protective activities or introduce unnecessary delays – how do you resolve conflicting interests?
- Some CERTs have the power to perform evidence collection, but prosecution is undertaken by other areas
- The role of CERTs is to provide technical expertise and facilitate coordination, LEAs undertake investigations and support prosecutions

- In some jurisdictions, CERTs refer all criminal activity to LEAs and will have limited interaction
- Some capability/responsibility limitations for CERTs and LEAs with regards to particularly sensitive issues such as SCADA.

Criminal Acts/Law Enforcement

- Varies according to jurisdiction with respect to;
    - Malware creation (illegal in some jurisdictions)
    - Retailing of exploits (illegal in many jurisdictions)
    - Use of exploits (illegal in all jurisdictions if used with criminal intent, some jurisdictions may allow use for educational purposes)
- Law enforcement use of transaction monitoring may support investigation/detection of malicious activity
- Some countries are still developing specific cyber security legislation and digital evidence alone may be insufficient to instigate proceedings in some jurisdictions

CERT Roles and Functions

- Some country's CERTs are just forming, others are more mature
- CERT role includes incident response, coordination, analysis and issuing of advisories
- Not all CERTs have a role in critical infrastructure protection or SCADA specific expertise
- Some CERTs have additional roles in cyber security awareness raising and training activities

Wrap up and Identified Capacity Building Priorities

17. Participants discussed the key observations amongst their table group and identified some priority areas for capacity building in the region. It was suggested that capacity building could focus on identifying training opportunities. Participants identified topics that they felt they could provide training to others in, as well as area's that they would like to receive additional training in. These are listed in the table below:

Topic identified by some participants as being able to provide training in:	Identified training needs that relate to topics (some are listed against more than one topic):
How to organise infrastructure in a secure manner	• Securing mobile devices (including issues surrounding "bring your own device" (BYOD)) • How to develop security policy for organisations • Exchanging experiences – case studies around incidents • Creating secure applications and web applications • Secure networks and webservers • Securing and configuring networks properly

Inside the criminal mind - how they build botnets, how they use botnets, how they find vulnerabilities, how they communicate	• Law enforcement training for CERTs to help CERTs better understand law enforcement issues • Monitoring and detecting malicious activity (less reliance on external feeds) • Digital forensics
Malware analysis and reverse engineering	• Malware analysis and reverse engineering • Monitoring and detecting malicious activity (less reliance on external feeds)
Digital Forensics	• Law enforcement training for CERTs to help CERTs better understand law enforcement issues • Digital forensics • Monitoring and detecting malicious activity (less reliance on external feeds)
Incident handling	• CERT training for law enforcement on technically specific subjects (such as control systems) • Exchanging experiences – case studies around incidents • Monitoring and detecting malicious activity (less reliance on external feeds) • Sharing incident response frameworks
Other identified training needs	• Integrating law/legislation and technology • Raising cyber security awareness at the international level (for example, model on the campaign to raise awareness for global warming) • Understanding different countries laws and regulations – similarities and differences • Cloud computing • What is already occurring within international cooperation (for example, Europe – ENISA) • General participant suggestion: future ARF workshops could also be scenario based, with participant countries asked to suggest scenarios to be discussed

18. The Co-Chairs concluded the workshop and thanked everyone for their active participation in the workshop. The intent of the workshop was to provide a practical avenue to explore the many issues the region faces in responding to cyber security incidents. It was highlighted that the workshop generated a number of observations and opportunities for future capacity building activities within the ARF.

Annex A – ARF Cyber Incident Response Workshop VOIP scenario

Scenario – VOIP

Part 1

Alarming amounts of call fraud are being reported by corporations in your jurisdiction. This is only happening in corporations that use virtual switching solutions (remotely configurable PBX).

Part 1 Discussion Questions

1. What mechanisms are there for organisations to report these incidents? Are there metrics kept for these incidents?
2. Who would do the initial analysis in this situation?
3. What is the role for the corporation?
4. What are the different roles for law enforcement, CERT's and regulators (telecommunications)?

Part 2

Indications are that compromised systems have been well configured and analysis has now shown that this incident is due to exploitation of a previously unknown vulnerability in widely used virtual PBX. Investigation activity identifies an online forum from a person retailing an exploit for this vulnerability. A number of different actors are known to be purchasing the weaponised exploit to perpetuate mass call fraud.

Part 2 Discussion Questions

1. Assuming the PBX vendor is based in your jurisdiction – how would you work with them with regards to the exploit?
2. Assuming the online forum was hosted in your jurisdiction – what action would be taken? What evidence needs to be collected under your legislation?
3. Assuming the purchasers of the exploit were located in your jurisdiction - what action would be taken?
4. Assuming the developer of the exploit was in your jurisdiction – what legal options are available to you?
5. What legislation, codes and practices could you enact to take forward the investigation?
6. How would you work with the vendor to resolve the situation?
7. What steps would you take to warn other users of that brand of PBX – both domestically and internationally?
8. What information would be required to pursue an investigation in to the developer and seller of the exploit? Are there any restrictions on disclosing information to relevant parties?
9. What factors influence sharing information, and the timing of sharing information on a vulnerability?
10. How do you work with industry to ensure that they have information when a patch becomes available?

Annex B – ARF Cyber Incident Response Workshop SCADA Vulnerability scenario

Scenario - SCADA Vulnerability

Part 1

At a hacker convention a group of vulnerability researchers have released a large number of high consequence, easy to exploit control systems product vulnerabilities; working exploits for these vulnerabilities have been packaged in an easy to use form. These control system products are used extensively in your jurisdictions critical infrastructure.

Part 1 Discussion Questions

1. Is the release of these vulnerabilities an offence? If the vulnerability is used, has an offence been committed by the user and/or the creator?
2. When would this be pursued? As the vulnerability is related to critical infrastructure systems are there different rules of engagement?
3. Who would you notify at this stage? (not knowing if the vulnerabilities have been utilised yet) Domestically and/or internationally?
4. Would you be able to identify who uses this product in your jurisdiction? If so, how?

Part 2

You've contacted the vendor and the vendor has informed you that they no longer support the product, it is too complex and uneconomical to fix as it is an end of life product. The vendor is in your jurisdiction.

Part 2 Discussion Questions

1. What action would you take?
2. Would your stakeholders utilise third party patches?
3. What advice would you provide your stakeholders?

Part 3

Through protracted negotiations the vendor has now finally agreed to release a patch.

There is also an impact on cross-border stakeholders – for example, a power station across the border that supplies power to your jurisdiction.

Part 3 Discussion Questions

1. Do you have the mechanisms in place to ensure cross-border stakeholders use the patch?
2. What policy frameworks are in place to ensure the patch is applied in your jurisdiction and in other jurisdictions you're dependent upon?

Annex C – ARF Cyber Incident Response Workshop DDOS scenario

Scenario – DDOS

Part 1

An Issue Motivated Group is publically threatening to target a large number of key internet infrastructure systems.

Part 1 Discussion Questions

1. Noting that the group is speaking publically, who has primacy in your jurisdiction on creating a media strategy? Would you publicly acknowledge the threat? Coordinate internationally?
2. What systems do you have in your jurisdictions that are critically dependant on the internet? Are there restrictions on the types of systems that can be connected to the internet?
3. As a table group – select the critical system that is the target of this threat.
4. Does the identified critical system have measures in place already? How do you assess the level of preparedness? What additional preparations would you advise them to make?
5. What capabilities of government or surge resources would you be willing to offer to assist critical systems?
6. What mechanisms do you have to detect less publically made threats?

Part 2

The threat has now been realised and the critical system that your table selected has been attacked.

Part 2 Discussion Questions

1. What capacity do you have to detect that an attack has occurred? Do you have mandatory reporting? Why/why not?
2. Is this considered a criminal act?
3. What is your ability to detect attack activation and command and control infrastructure?
4. Command and control is identified as being hosted within your jurisdiction – what action would you take? Who would take this action?
5. Command and control is identified as being hosted outside of your jurisdiction (while the critical system being attacked is within your jurisdiction) – what action would you take? Who would take this action?
6. Technical response – what is the difference between the CERT response and the law enforcement response? What are the challenges? How could a policy framework integrate the differences? What approaches could be used to create a better integration in these areas?
7. Strategic response – what strategic initiatives could address this?